(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 September 2003 (04.09.2003)

PCT

(10) International Publication Number
WO 03/073707 A1

(51) International Patent Classification[7]: H04L 12/56, 12/46

(21) International Application Number: PCT/SE03/00326

(22) International Filing Date: 27 February 2003 (27.02.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0200640-1 28 February 2002 (28.02.2002) SE

(71) Applicant (*for all designated States except US*): **TELEFONAKTIEBOLAGET LM ERICSSON** (publ) [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors; and
(75) Inventors/Applicants (*for US only*): **BACKMAN, Jan** [SE/SE]; Floragatan 2, S-442 32 Kungälv (SE). **NORLUND, Krister** [SE/SE]; Engdahlsgatan 6 C, S-412 59 Göteborg (SE). **ENGSTRÖM, Anders** [SE/SE]; Volrat Thamsgatan 7 D, S-412 60 Göteborg (SE). **MAGNUSSON, Linus** [SE/SE]; Lindströmsgatan 3A, S-412 61 Göteborg (SE). **KÖPMAN, Johan** [SE/SE]; Arvid Lindmansgatan 6D, S-417 26 Göteborg (SE).

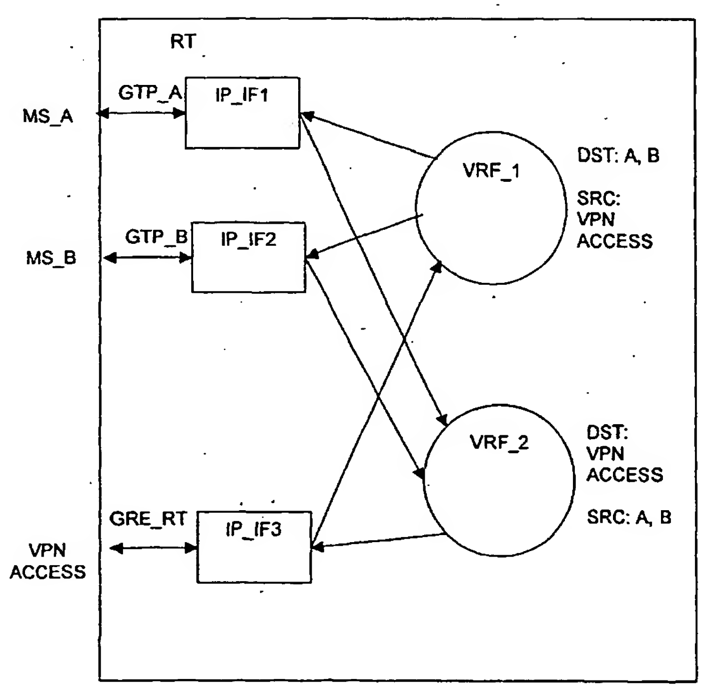
(74) Agent: **ERICSSON AB**; Patent Unit Radio Networks, S-431 84 Mölndal (SE).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: ROUTING IN VIRTUAL PRIVATE NETWORK



(57) Abstract: A network comprising a gateway GPRS support node (GGSN) serving at least one virtual private network (VPN), whereby the gateway GPRS support node comprises at least two virtual private network (VPN) routing/forwarding instances per internet protocol (IP) interface has been shown. A router with directional specific properties has moreover been disclosed.

WO 03/073707 A1

Published:
— *with international search report*

Routing in virtual private network

Field of the invention

The invention relates to the technical field of TCP/IP routing and forwarding and relates especially to concepts within virtual private networks (VPNs).

The main applications for the invention are IP routers with high VPN scalability demands, such as the GGSN (Gateway GPRS Switching Node) in GPRS (General Packet Radio Service) networks. The invention relates to WPP 5.0 (Wireless Packet Platform).

Background of the invention

A Virtual Private Network (VPN) is an extension to a network that is remotely administrated. This network is carried over the local network via tunnelling, either in protocols that either can be IP based or not IP based (for example ATM). When extending these networks into mobile packet data networks, a single node must handle a large number of VPNs. This implicates that the management and configuration of all these extensions to the VPNs has to be managed by the operator managing the mobile packet network. In for example GPRS (General Packet Radio Service), the GGSN (Gateway GPRS Switching Node) connects the mobile network to the remotely administrated network. Figure 1 depicts a schematic overview of such a GPRS network with the GGSN.

Figure 2 depicts an example with traffic between two mobile stations. This example shows that the administrator of the GGSN has to manage the packet filtering rules that protects the mobile stations from each other. The traffic between mobile stations cannot be monitored from a remotely administrated network.

One known solution is based on an implementation of packet filtering doing packet forwarding. By defining a packet filter that forwards all traffic from one interface or tunnel to another interface or tunnel, the routing information in the forwarding table will not be considered and the traffic can be forced to a remote network.

Another known WPP solution to the problem is to directly map traffic from one interface/tunnel into another interface or tunnel, without making a forwarding decision

based on the destination IP address. This known solution is called APN (Access Point Name) Routing.

The disadvantage with the above solutions is poor redundancy, since the packet filters (or mapping table) are not dynamically updated and the interface or tunnel that the packets are forwarded to might be unavailable due to link or network problems.

Fig. 3 shows two nodes A and B and a router R being physically connected to an Ethernet segment ETH S. Two virtual private networks VPN_1 and VPN_2 are implemented over the common Ethernet segment ETH_S. Node A comprises a first and a second IP interface IP_IF1 and IP_IF2. The IP interfaces IP_IF1 and IP_IF2 at the IP layer 3 are mapped to the given unique layer 2 MAC (Media Access Control) Ethernet address ETH_IF1 by means of the ARP (automatic Request Protocol) protocol.

Likewise interfaces IPIF3 and IP_IF4 are mapped to Ethernet interface ETH_IF2 of node B. IP interfaces IP_IF5 and IP_IF6 is mapped to ETH_IF2 on router RT.

IP_IF1 of node A forms a first virtual private network VPN_1 with IP_IF3 of node B. IP_IF4 of node B forms a second virtual private network VPN_2 with IP_IF6 of router RT. IP Packets may be communicated between the respective IP interfaces over the respective VPN's. To the various IP interfaces of each respective VPN it appears that the Ethernet segment is exclusive.

Fig. 4 shows an exemplary IP packet delivered from IP interface IP_IF3 to IP_IF1 on VPN_1 for the network shown in fig. 3. The IP packet is encapsulated in an Ether packet with source address ETH_IF2 and destination address ETH_IF1. It has an Ethernet type identification of type "VLAN" – Virtual Local Area Network – and carries a corresponding network identifier VPN_1 and a second Ethernet type identifier IPv4 pertaining to the version of the IP protocol being used. In the Ethernet payload ETH_PL there is provided the IP source and destination addresses mentioned above and the IP payload. The packet is ended by an Ethernet cyclical redundancy check value ETH CRC.

In fig. 5 an exemplary prior art network has been shown comprising a router RT providing a first virtual private network VPN_1 via forwarding table VRF_1 providing interconnectivity for IP interfaces IP_IF1, IP_IF2 and IP_IF3. The router moreover

provides a second virtual private network VPN_2 via forwarding table VRF_2 providing interconnectivity for IP interfaces IP_IF5 and IP_IF6.

Summary of the invention

It is first object of the invention to set forth a router that allows for selective routing depending on traffic direction.

This object has been accomplished by claim 1.

It is a secondary object to set forth a router that allows for communication between various private networks.

This object has been accomplished by claim 2.

It is a third object to set forth a system allowing for forced traffic over a specific interface.

This object has been accomplished by claim 6.

It is a fourth object to set forth a system in which packet control is deferred to a corporate network.

This object has been accomplished by claim 7.

According to a further aspect of the invention, in order to increase the security in a VPN network it is desired that all traffic (i.e. IP packets) from mobile terminals always shall go via the home network. This gives the VPN administrator the possibility to specify the packet filtering rules to be applied both for traffic destined to a mobile terminal, as well as for traffic coming from a mobile terminal. This is independent of whether the packets are destined to the same mobile network extension as the packet originated from, or not. Without forcing traffic to the home network, the packet filtering rules would have to be configured by the operator of the mobile extension to the VPN network instead of the administrator of the home network.

Further advantages of the invention will appear from the following detailed description of preferred embodiments of the invention.

Brief description of the drawings

Fig. 1 shows an overall diagram of the GPRS network architecture,

fig. 2 shows a known method of performing routing in a GPRS network,

fig. 3 shows a known way of implementing virtual private networks (VPN) on an Ethernet segment,

fig. 4 shows a packet used in fig. 3,

fig. 5 shows a prior art router providing two VPN networks,

fig. 6 shows a first embodiment of a router according to the invention,

fig. 7 shows a second embodiment of a VPN network according the invention including a packet flow form a node A to a node B,

fig. 8 shows the same VPN network as in fig 7, including a packet flow form a node B to a node A,

fig. 9 shows an application of the present invention in a GPRS network, and

fig. 10 shows a fourth embodiment according to the invention.

Detailed description of preferred embodiments of the invention

According to the invention, multiple VRF's (VPN Routing/Forwarding instances) are used per IP interface. An IP interface can for example be a bi-directional IP-in-IP tunnel or an IP-over-Ethernet interface. The forwarding table that is used to route traffic from a given

interface may not route traffic to the same IP interface. This distinction makes it possible to let traffic in one direction belong to one VRF and traffic in the other direction belong to another VRF. Furthermore, if the interface has multiple peers, each peer end-point can belong to different VRF's.

Fig. 6 shows a first embodiment of the invention, comprising a router RT comprising router tables VRF_1 and VRF_2 and IP interfaces IP_IF1, providing access to a GTP tunnel GTP_A, which connects to a first mobile station MS_A and IP interface IP_IF2, providing access to a second GTP tunnel GTP_B that connects to mobile station MS_B. The router moreover comprises a third IP interface IP_IF3 that connects to GRE tunnel GRE_RT providing connection to a VPN access net, such as a corporate Intranet.

As indicated by the arrows, forwarding table VRF_1 routes packets form IP interface IP_IF3 to IP interface IP_IF1 and IP_IF2 depending on which mobile station the given packet is intended for. Forwarding table VRF_2 route packets from source MS_A and MS_B to IP interface IP_IF3 and further to the VPN access net. Thereby, the traffic between mobile stations MS_A and MS_B can be controlled by the VPN access net.

Fig. 7 shows a further embodiment of the invention in which a first router RT connects to an Ethernet segment ETH_S via IP interfaces IP_IF1, IP_IF2 and IP_IF3, forming respective virtual private networks VLAN1, VLAN2 and VLAN3 and an Ether router interface ETH_IF. The first router comprises a first forwarding table VRF_1 and forwarding table VRF2.

A node A connects to the router via virtual local area network VLAN1 and a node B connects to the router via virtual local network VLAN2 over the common Ethernet segment ETH_S.

A second router R comprising forwarding table VRF_T connects VLAN3 over the common Ethernet segment ETH_S. The second router also connects to the Internet.

Forwarding tables VRF_1 defines for destination A a next hop of IP interface IP_IF1 and for destination node B IP interface IF2. Forwarding tables VRF_2 defines interface IP_IF3 as default next hop address. Forwarding table VRF_R defines IP interface IPIF_3 for both destinations A and B.

A packet sent from mobile station A to B is forwarded along arrow 10 through IP interface IPIF_1 to forwarding table VRF_2 and further on to IP interface IPIF_3 to router R, arrow 20, and back again to IP interface IPIF_3 and to forwarding table VRF_1. Forwarding table VRF_1 defines IP interface IPIF_2 as next hop for destination B, and consequently the packet is transmitted to node B along arrow 30.

The router is being configured such that in the event that a mobile station on one interface IP_IF1 is communicating with a mobile station on interface IP_IF2, the traffic may be routed via the second interface IP_IF3.

In fig. 8 the opposite path of transmitting a packet has been shown as indicated by arrows 40, 50 and 60.

It should be understood that the many other technologies that Ethernet could be used on the data link layer.

As shown above, the forwarding table for a VRF can only have routes to interfaces that in the outbound direction belong to the VRF. The question of which VRF to use for the forwarding decision is selected from the VRF configuration for the inbound direction of the receiving interface. The definition of interfaces in both outbound and inbound direction can be extended to also consider the source and destination peers (can for instance be identified via link level addresses) to allow different VRFs for different remote peers (for example routers) on a multi-access link.

The distinction between inbound and outbound direction provides the possibility that an interface can be used by multiple VRFs in the outbound direction. That is, several VRFs can use the same outbound link. In figure 7, it is shown how both VRF_1 and VRF_2 use the same outbound link, for instance IPIF_3. This feature is very useful together with broadcast and multicast based services. One example is that it makes it possible to have a separate multicast VPN that gives multicast services that several other VPNs can use. Traffic from the multicast network can be forwarded into another VPN where the end-users of the service are connected. The benefit of doing this is that the common services between the networks can use one common network architecture that enables more efficient use of the transport links. This is how multicast networks are used to give better performance, but multicast services are currently not possible to share between VPNs and this invention provides a solution to the problem.

The main problem in WPP solved by the invention is that it allows GGSN nodes to defer packet filtering to a remote network to decrease the need of packet filtering configurations for the manager of the GGSN node. The present invention provides a scalable routing solution towards the external networks.

Figure 9 depicts a third preferred embodiment of the invention in which traffic between two mobile stations MS#1 and MS#2, belonging to the same corporate network as the router holding VRF#23, according to the invention. VRF#37 and VRF#42 are used in the GGSN and VRF#23 is used in the router. The invention is used in the GGSN. For traffic from the mobile stations VRF#42 is used. For traffic from the router VRF#37 is used. VRF#42 has the Router as next hop for all the routes in the forwarding table. This means that all traffic from the mobiles is sent to the router. VRF#37 has the SGSN (Serving GPRS Support Node) as next hop for the two mobile stations. This means traffic from the Router destined to the Mobile Stations are sent to the SGSN. Traffic from the router which is not destined to the Mobile Stations are sent back to the router as the forwarding table for VRF#37 has an default route pointing out the router as next hop for all traffic which is not destined to the mobile stations. The router only has one VRF (VRF#23) for all its interfaces. The router is a normal router. A packet sent from one of the mobile station destined to the other mobile station is sent to the GGSN via the SSGN. The GGSN performs a forwarding lookup (using the forwarding table of VRF#42) and then routes the packet to the router. The router performs a forwarding lookup and routes the traffic back to the GGSN as the forwarding table for VRF#23 points out the GGSN as next hop for the mobile stations. The GGSN once again makes a forwarding lookup (using the forwarding table of VRF#37) and then routes the packet to the SGSN. The SGSN delivers the packet to the receiving mobile station. It should be noted that, a third mobile station not belonging to the corporate network would not use the tunnel shown in fig. 3. Another parallel set of tunnels and forwarding tables would be set up.

Figure 9 shows an example of how the Network Management responsibilities can be divided between different administrators. In this figure, the mobile stations MS#1, MS#2 and the router holding VRF#23 belong to the same corporate network, designated "Corporate", and all administration for this network is handled by the corporate network administrator. By way of example, a first operator, Operator 1, controls the SGSN node and a second operator, Operator 2, controls the GGSN node. There is a clear separation between GPRS network administration and the administration of the corporate network.

This example also shows, when applicable, the separation between the SGSN and GGSN operators. It is a strong business case for an operator to provide the corporate networks with a service, making it possible for the corporate network administrator to configure the packet filters for the mobile stations and monitor all traffic to and from mobile stations. It is therefore a strong business case for a GGSN vendor to provide an operator with equipment implementing this invention. It should be noted that forwarding tables VRF#37 and VRF#42 are controlled by Operator 2 in accordance with whatever agreement exists between Corporate and Operator 2.

The ability to route packets to the VRF in the opposite direction for an interface have been implemented. This is necessary to implement, if ICMP messages shall be supported. The VRF for the opposite direction is easy to find, since ICMP messages are generated for an outbound interface and the packet can then be handled as if it had arrived on that interface. The forwarding table in a VRF can be updated by a routing daemon.

Routing daemons receive their routing information from different interfaces and can treat these interfaces as belonging to different routing areas. By separating the inbound and outbound direction of these interfaces, the routing protocol can be configured to filter which information to send to different interfaces. Thereby, the directions of the routing updates can be separated; if the routing protocol used for route announcements supports unidirectional links.

The invention can for example be used for IPv4 and IPv6. Both IPv4 and IPv6 interfaces can be bi-directional or unidirectional. The present invention provides the possibility for a router (or host) to treat bi-directional interfaces as two uni-directional interfaces at the same time as the peer routers (or hosts) view the interface on the router (or host) as a bi-directional interface. In other words, the surrounding network environment is not affected by the use of the invention, if it is not deliberately used in such a way.

The invention has a high potential to solve many current and future problems in different areas of IP routing, since it is a fundamental change of how interfaces are treated in IP routing and forwarding environments.

Abbreviations

ATM	Asynchronous Transfer Mode
APN	In the GPRS backbone, an Access Point Name (APN) is a reference to a GGSN. To support inter-PLMN roaming, the internal GPRS DNS functionality is used to translate the APN into the IP address of the GGSN.
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
ICMP	Internet Control Message Protocol (RFC 792)
IP	Internet Protocol (RFC 791)
IP IF	IP interface
SGSN	Serving GPRS Support Node
TCP	Transmission Control Protocol (RFC 793)
TCP/IP	Suite of protocols, including IP, TCP UDP, ICMP and other protocols
UDP	User Datagram Protocol (RFC 768)
UMTS	Universal Mobile Telephone System
VPN	Virtual Private Network.
VRF	VPN Routing/Forwarding instance
WPP	Wireless Packet Platform

Patent claims

1. Router (RT) comprising at least two IP interfaces (IPIF_1; IPIF_2; IPIF_3), whereby each IP interface is associated with a respective virtual private network (VPN1; VPN2; VPN3), the router moreover comprising at least two forwarding tables (VPF_1; VPF_2),

whereby a first table (VPF_1; VPF2) is used for routing traffic towards a given interface (IPIF1; IPIF2; IPIF3), and

the second table (VPF_2; VPF1) is used for routing traffic appearing from the same given interface (IPIF_1; IPIF_2; IPIF_3).

2. Router according to claim 2, wherein packets received on one IP interface (IPIF_1; IPIF_2; IPIF_3) and relating to one given virtual private network (VPN1; VPN2; VPN3) is forwarded to another IP interface (IPIF_1; IPIF_2; IPIF_3) relating to another virtual private network (VPN1; VPN2; VPN3).

3. Router according to any previous claim whereby a first IP interface (IP_IF1) is coupling to a first tunnel (GTP_A) providing bi-directional connectivity to mobile stations and a second IP interface (IP_IF3) is coupling to a tunnel (GRE_RT) providing bi-directional connectivity to a corporate network.

4. Router according to claim 3, comprising a third interface (IP_IF2) providing bi-directional connectivity to mobile stations, the router being configured such that in the event that a mobile station on one interface (IP_IF1) is communicating with a mobile station on a third interface (IP_IF2), the traffic is routed via the second interface (IP_IF3).

5. Router according to claim 4, wherein the packets from one mobile station (MS_A) to another mobile station (MS_B) is forwarded to a remote router (R), the remote router being adapted for taking a policy decision, such as to discard packets.

6. Network comprising a router (RT) comprising at least two IP interfaces (IPIF_1; IPIF_2; IPIF_3), whereby each IP interface is associated with a respective virtual private network (VPN1; VPN2; VPN3), the router moreover comprising at least two forwarding tables (VPF_1; VPF_2),

   whereby a first table (VPF_1; VPF2) is used for routing traffic towards a given interface (IPIF1; IPIF2; IPIF3) and the second table (VPF_2; VPF1) is used for routing traffic appearing from the same given interface (IPIF_1; IPIF_2; IPIF_3),

   wherein packets received on one IP interface (IPIF_1; IPIF_2; IPIF_3) and relating to one given virtual private network (VPN1; VPN2; VPN3) is forwarded to another IP interface (IPIF_1; IPIF_2; IPIF_3) relating to another virtual private network(VPN1; VPN2; VPN3),

   whereby a first IP interface (IP_IF1) is coupling to a first tunnel (GTP_A) providing bi-directional connectivity to mobile stations and a second IP interface (IP_IF3) is coupling to a tunnel (GRE_RT) providing bi-directional connectivity to a corporate network, and whereby a third interface (IP_IF2) is providing bi-directional connectivity to mobile stations, the router being configured such that in the event that a mobile station on the first interface (IP_IF1) is communicating with a mobile station on the third interface (IP_IF2), the traffic is routed via the second interface (IP_IF3).

7. Network according to claim 6 comprising a remote router, being configured such that packets from one mobile station (MS_A) to another mobile station (MS_B) is forwarded to said remote router (R), the remote router selectively taking a policy decision, such as to discard packets.

8. Network according to claim 7, wherein the remote router comprising a firewall.

9. Network according to claim 6, wherein the router (RT) is comprised in a GGSN node.

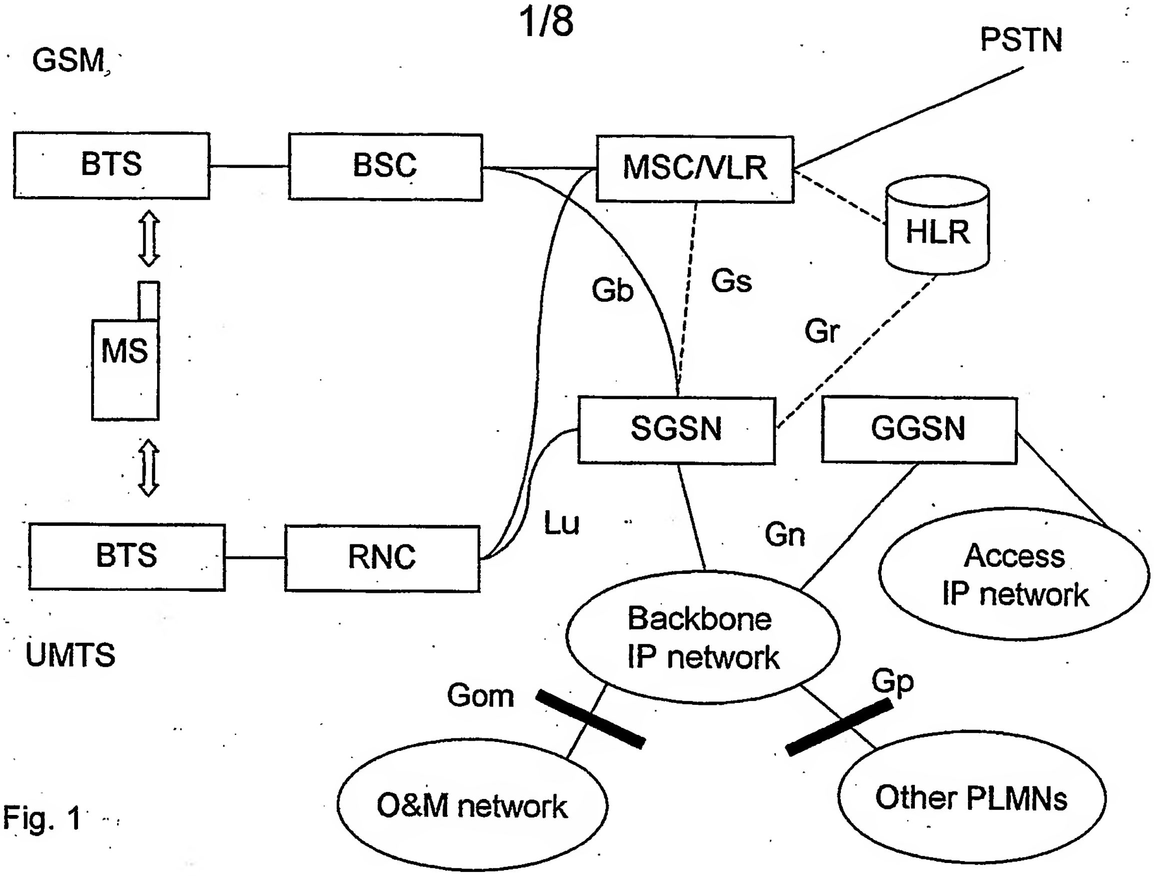

GSM
PSTN
BTS
BSC
MSC/VLR
HLR
MS
Gb
Gs
Gr
SGSN
GGSN
BTS
RNC
Lu
Gn
Access
IP network
Backbone
IP network
UMTS
Gom
Gp
O&M network
Other PLMNs

Fig. 1

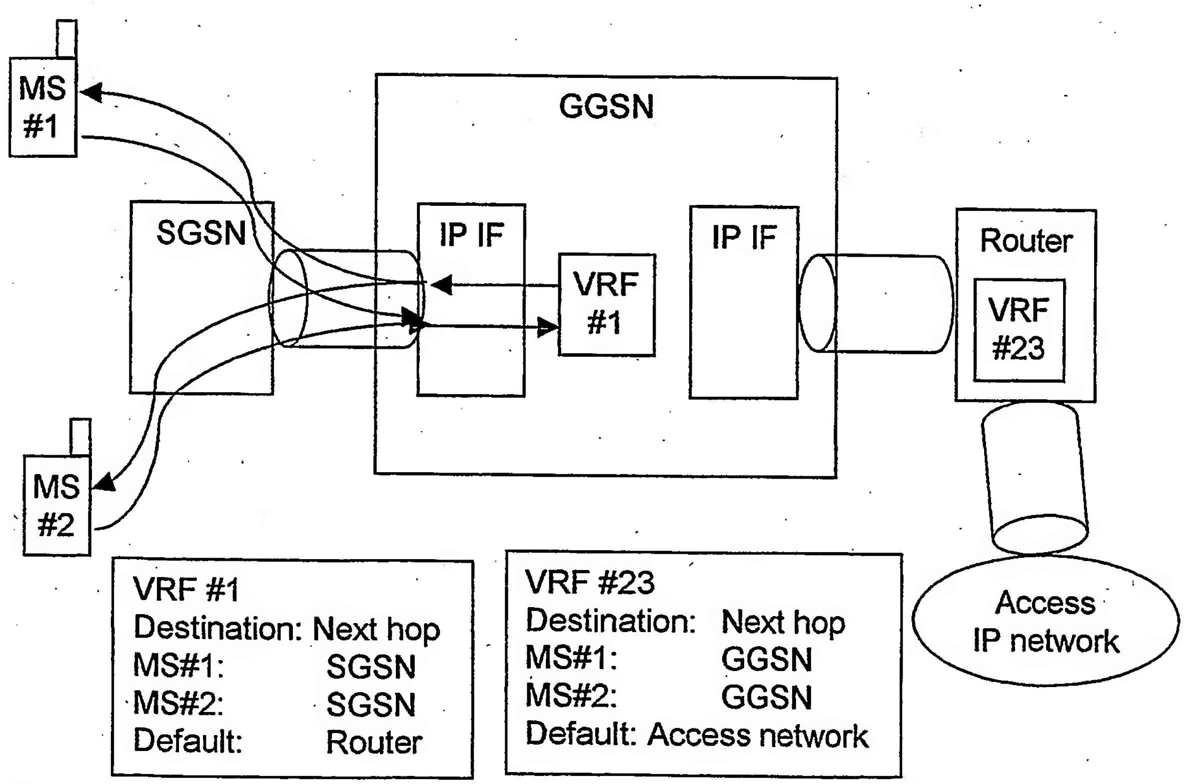

MS
#1
GGSN
SGSN
IP IF
IP IF
VRF
#1
Router
VRF
#23
MS
#2
Access
IP network
VRF #1
Destination: Next hop
MS#1: SGSN
MS#2: SGSN
Default: Router
VRF #23
Destination: Next hop
MS#1: GGSN
MS#2: GGSN
Default: Access network

Fig. 2

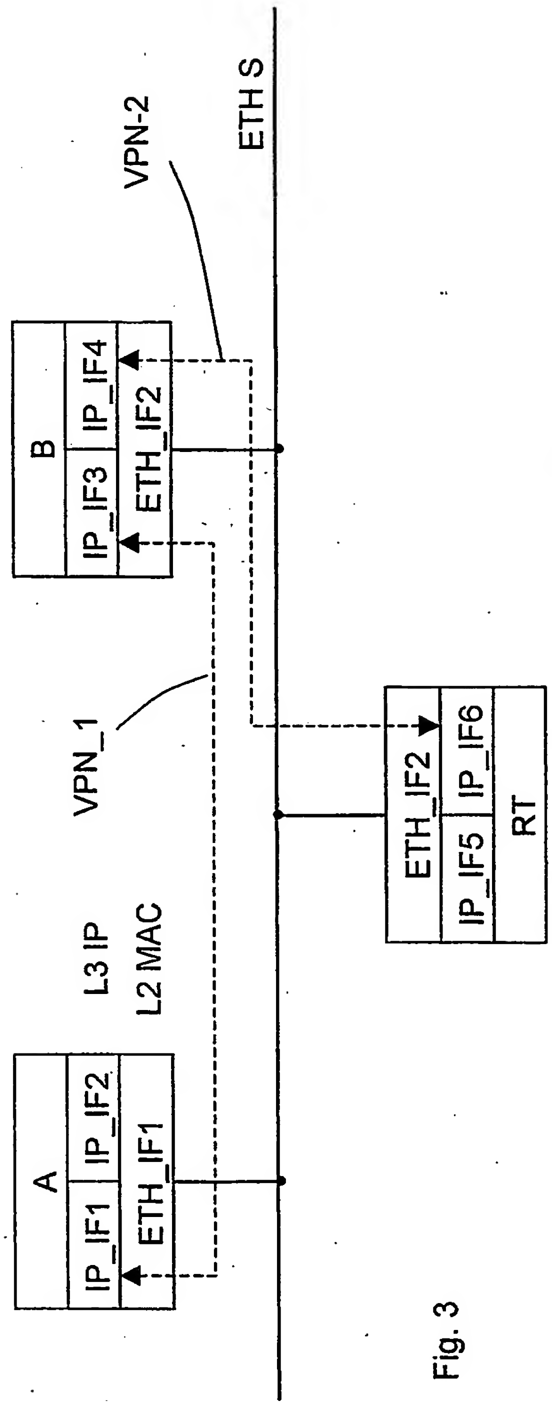

A
IP_IF1
IP_IF2
ETH_IF1
B
IP_IF3
IP_IF4
ETH_IF2
ETH_IF2
IP_IF5
IP_IF6
RT
L3 IP
L2 MAC
VPN_1
VPN-2
ETH S

Fig. 3

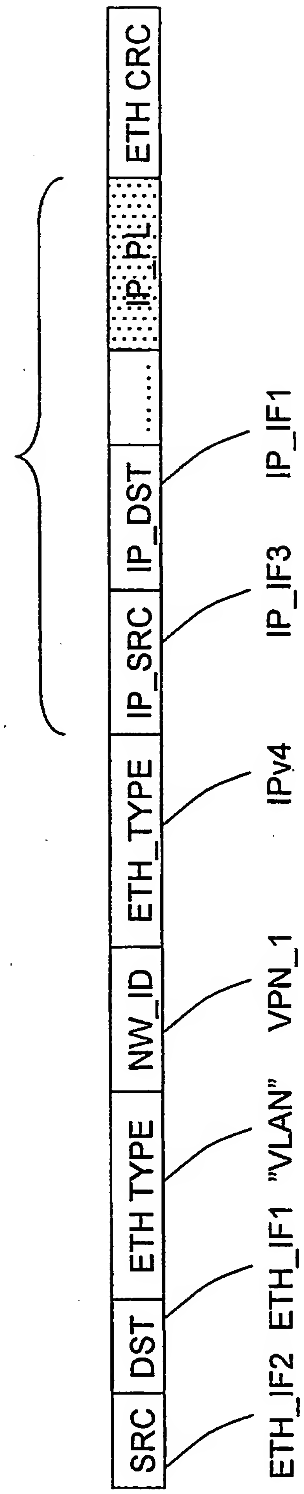

SRC
DST
ETH TYPE
NW_ID
ETH_TYPE
IP_SRC
IP_DST
....
IP_PL
ETH CRC
ETH_PL
ETH_IF2
ETH_IF1
"VLAN"
VPN_1
IPv4
IP_IF3
IP_IF1

Fig. 4

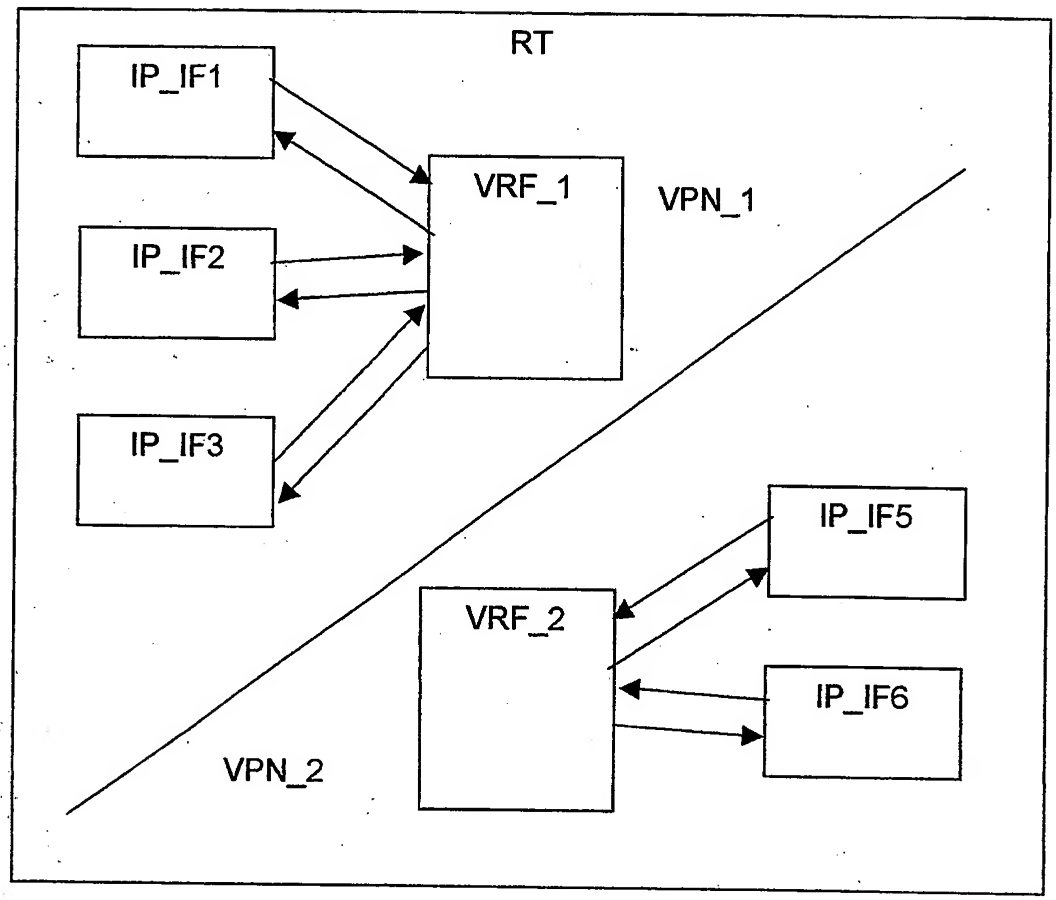


Fig. 5 - Prior art

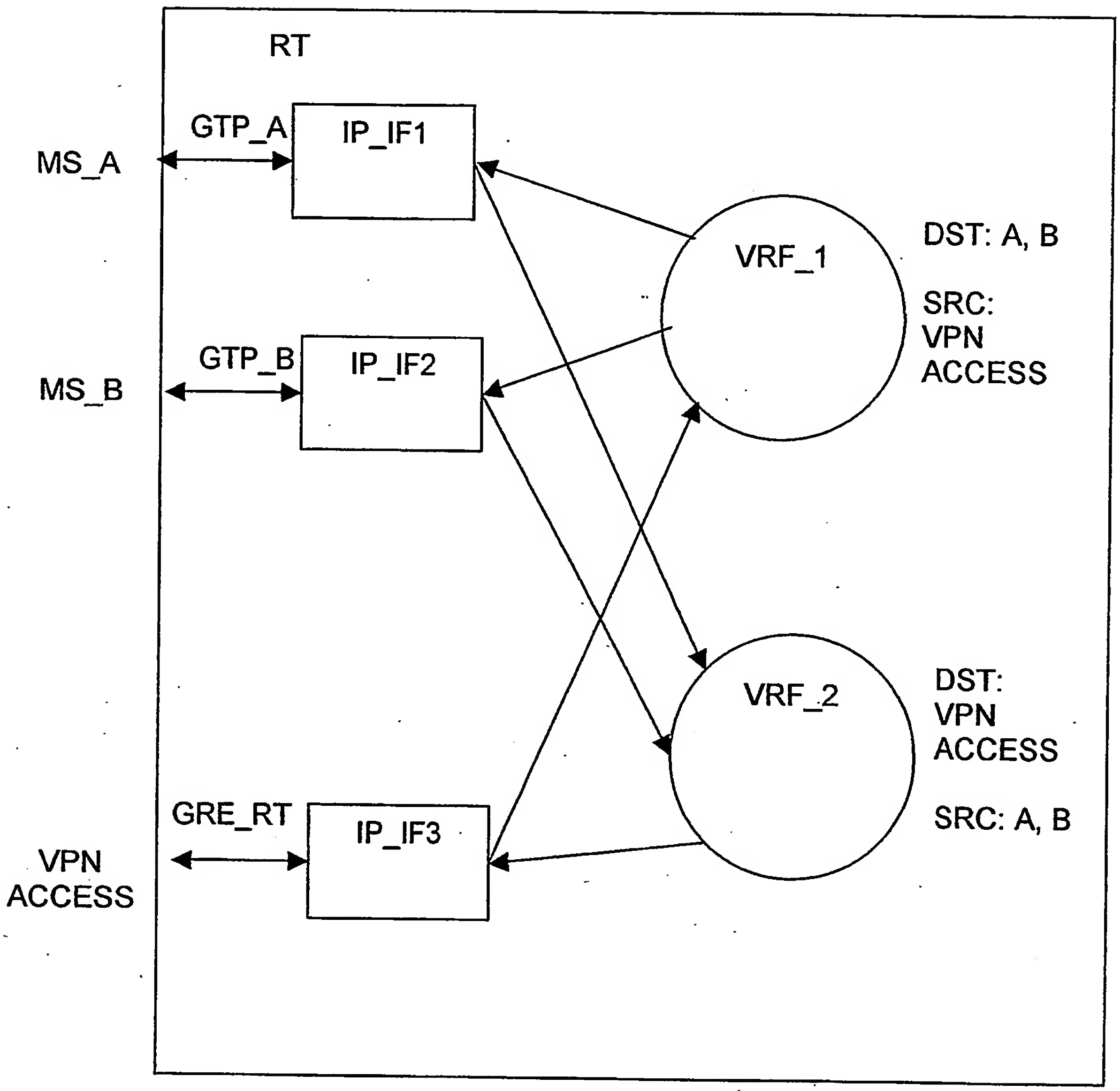

RT
GTP_A
IP_IF1
MS_A
VRF_1
DST: A, B
SRC:
VPN
ACCESS
GTP_B
IP_IF2
MS_B
VRF_2
DST:
VPN
ACCESS
SRC: A, B
GRE_RT
IP_IF3
VPN
ACCESS

Fig. 6

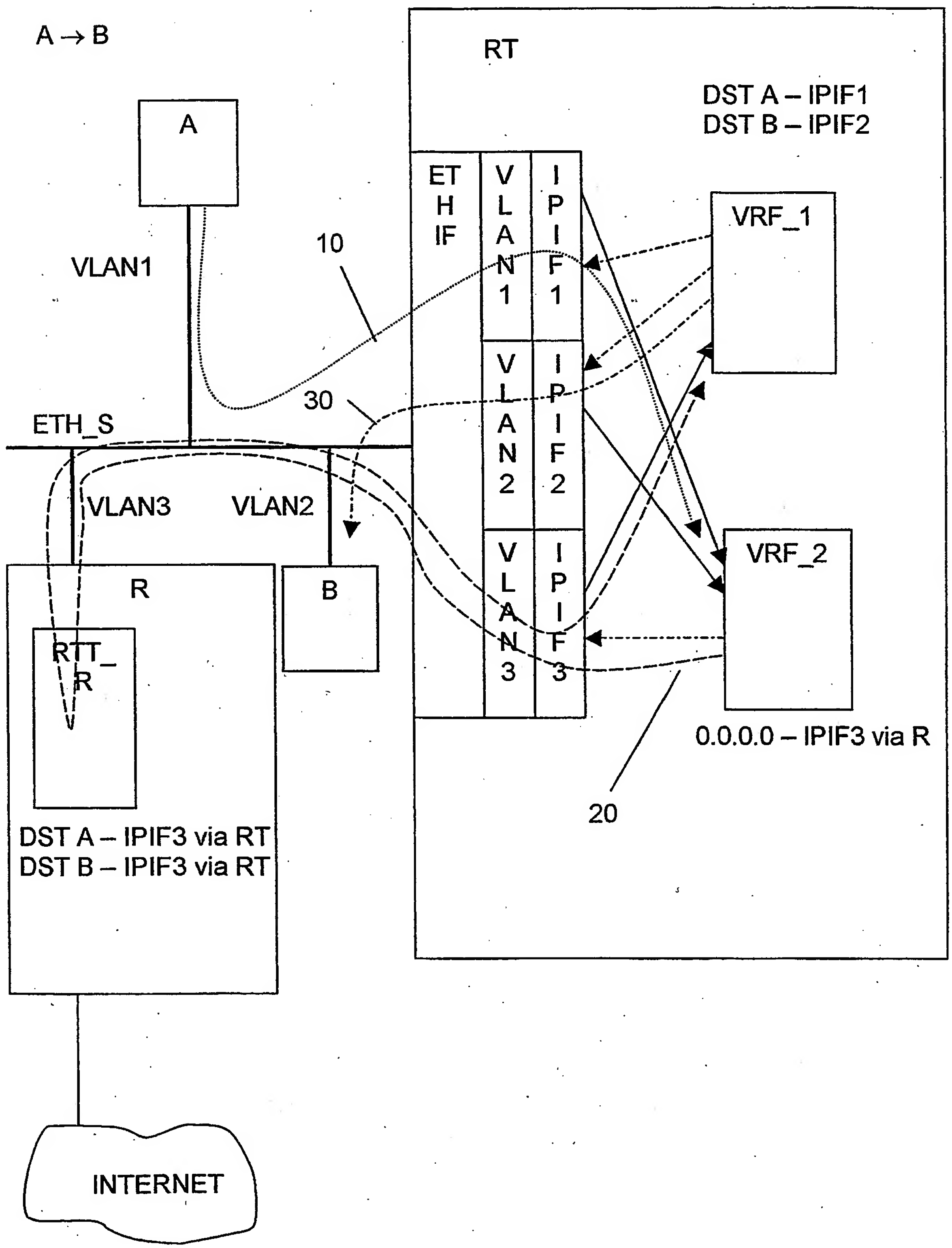

A → B
RT
DST A – IPIF1
DST B – IPIF2
A
ET H IF
V L A N 1
I P I F 1
VRF_1
10
VLAN1
30
V L A N 2
I P I F 2
ETH_S
VLAN3
VLAN2
V L A N 3
I P I F 3
VRF_2
R
B
RTT_R
0.0.0.0 – IPIF3 via R
20
DST A – IPIF3 via RT
DST B – IPIF3 via RT
INTERNET

Fig. 7

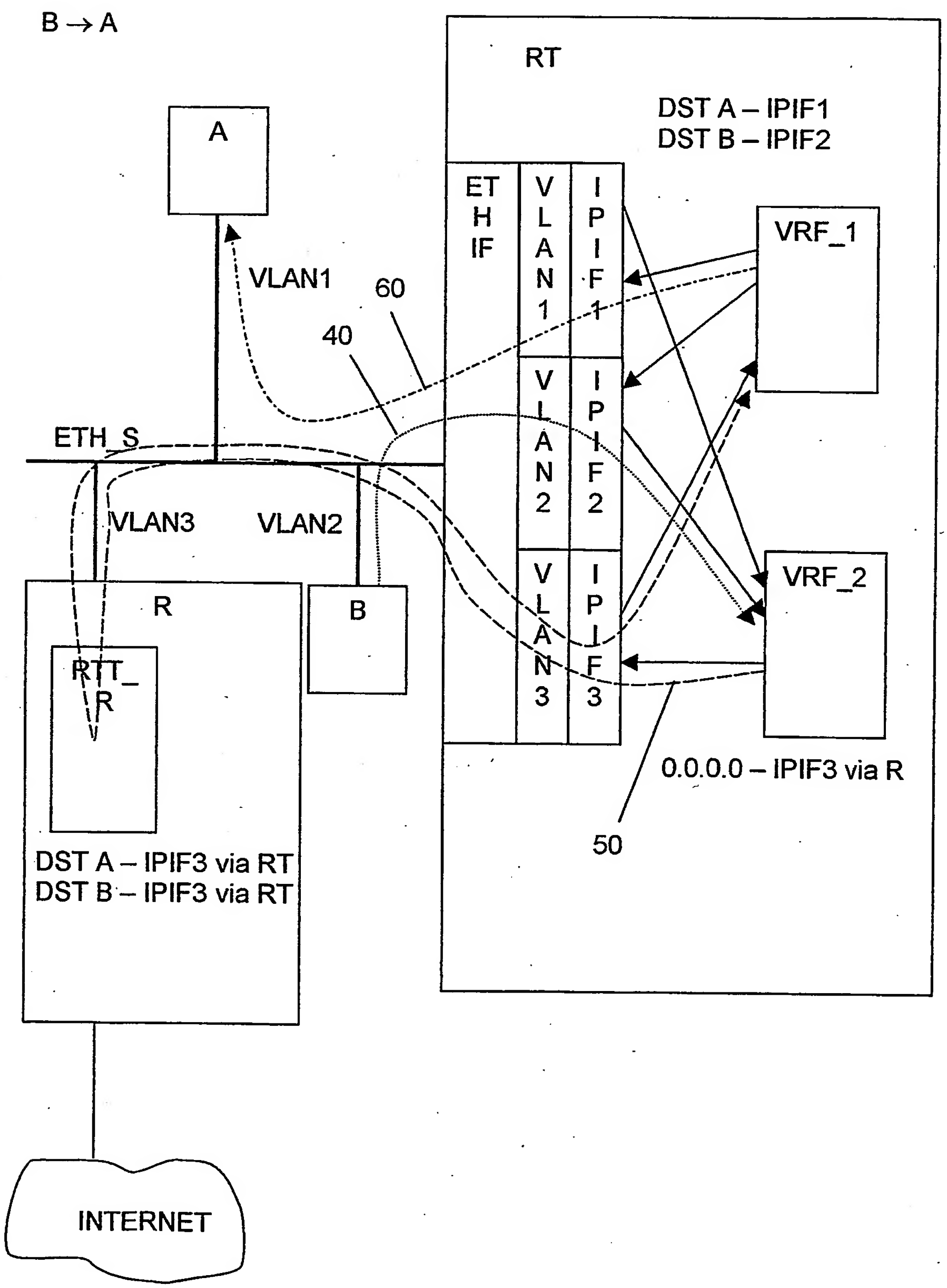
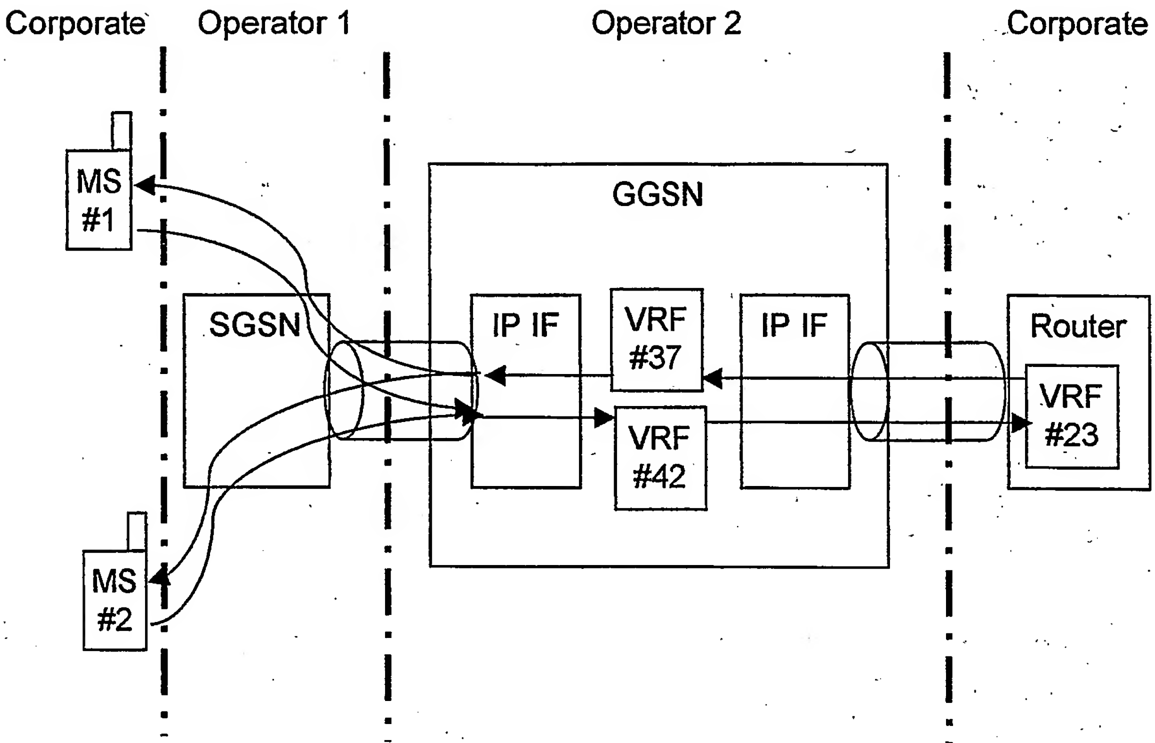

B → A
RT
DST A – IPIF1
DST B – IPIF2
ETH IF
VLAN1
IPIF1
VLAN2
IPIF2
VLAN3
IPIF3
VRF_1
VRF_2
A
VLAN1
60
40
ETH_S
VLAN3
VLAN2
R
B
RTT_R
0.0.0.0 – IPIF3 via R
50
DST A – IPIF3 via RT
DST B – IPIF3 via RT
INTERNET

Fig. 8

VRF #23	
Destination:	Next hop
MS#1:	GGSN
MS#2:	GGSN
Default:	Access network



VRF #42	
Destination:	Next hop
MS#1:	Router
MS#2:	Router
Default:	Router

VRF #37	
Destination:	Next hop
MS#1:	SGSN
MS#2:	SGSN
Default:	Router

Fig. 9

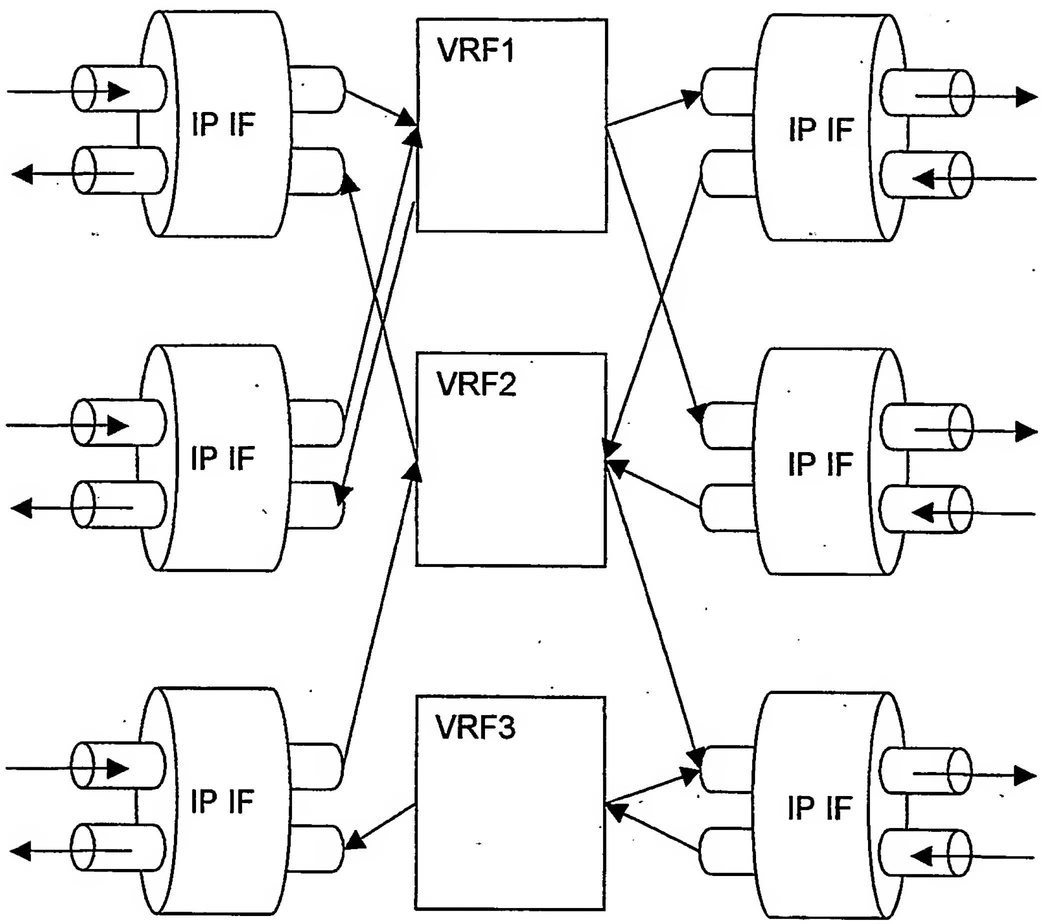


Fig. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 03/00326

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 12/56, H04L 12/46

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ROSEN, E. et al., March 1999. Network Working Group. Request for Comments: 2547. Category: Informational. See chapters 1-3 --	1-9
A	US 2002181477 A1 (MO, L. ET AL), 5 December 2002 (05.12.02), [3]-[10] --	1-9
A	EP 1071296 A1 (ALCATEL), 22 July 1999 (22.07.99), figure 3 --	1-9

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 April 2003	20-05-2003

Name and mailing address of the ISA/	Authorized officer
Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Anders Edlund /LR Telephone No. +46 8 782 25 00

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Mobile VPNs for Next Generation GPRS and UMTS Networks. White Paper, Lucent Technologies, Bell Labs Innovations, publ. 2000. See the entire document -- --------	1-9

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002181477 A1	05/12/02	WO 02098046 A	05/12/02
EP 1071296 A1	22/07/99	AU 4262200 A	25/01/01
		CA 2313984 A	22/01/01
		JP 2001077859 A	23/03/01